



JOHN NAIMO
AUDITOR-CONTROLLER

COUNTY OF LOS ANGELES DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

October 5, 2015

TO: Mitchell H. Katz, M.D., Director
Department of Health Services

FROM: John Naimo 
Auditor-Controller

SUBJECT: **HIPAA AND HITECH ACT PRIVACY COMPLIANCE REVIEW –
WILMINGTON HEALTH CENTER**

We have completed a review of the Department of Health Services (DHS) Wilmington Health Center's (Wilmington) compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic Clinical Health (HITECH) Act.¹

On August 18, 2015, we provided your Department with our final draft report. Wilmington staff generally agreed with our findings and recommendations, and indicated that a formal exit conference was unnecessary.

Approach/Scope

Our approach and scope considered that Wilmington is an outpatient facility with a focus on disease prevention, immunizations, prenatal care, women's health, and wellness. The facility houses approximately 40 workforce members and has an onsite pharmacy. Wilmington is part of DHS' Coastal Ambulatory Care Network (Coastal), which also includes the Long Beach and Bellflower Health Centers. All three health centers are subordinate to the Ambulatory Care Network (ACN) for administrative and clinical oversight and Harbor-UCLA Medical Center (Harbor-UCLA) for facilities support and ancillary services.

On May 7, 2015, we conducted a comprehensive onsite review to evaluate Wilmington's compliance with the HIPAA Privacy Rule and DHS' HIPAA policies and procedures that are pertinent to an outpatient facility. We met with DHS' Privacy Officer, Wilmington's

¹ 45 Code of Federal Regulations (CFR) Parts 160 and 164

Administrative Clinic Manager, and ACN Coastal Health Centers' Privacy Coordinator and Health Information Management Director (Privacy Coordinator). We utilized the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Program Check List/Audit Tool* in evaluating Wilmington's compliance with the HIPAA Privacy Rule and DHS' HIPAA Privacy Rule policies and procedures. DHS management is responsible for establishing and maintaining effective internal compliance with the HIPAA regulations, and has oversight of the HIPAA program throughout their facilities, including Wilmington. We considered DHS' internal controls over their compliance program, DHS policies, and the HIPAA Privacy Rule requirements that could have a direct and material effect on Wilmington.

Our review covered the Privacy Rule requirements for:

- Notice of privacy practices (NPP) for protected health information (PHI)
- Safeguards for PHI
- Training
- Complaint process
- Uses and disclosures requiring authorization
- Refraining from intimidating or retaliatory acts
- Accounting of disclosures of protected health information
- Minimum Necessary Rule
- HITECH Act breach notifications
- Appropriate access to ePHI
- Contingency plan
- Proper disposal/destruction of PHI

Our review also examined, on a limited basis, Wilmington's compliance with certain aspects of the Security Rule where there was cross-over with the Privacy Rule. These included administrative, physical, and technical safeguards. To assist us with this onsite review, we met with DHS' Privacy Officer, as well as the Coastal Health Centers' Privacy Coordinator and Wilmington staff.

Results of Review and Recommendations

Notice of Privacy Practices For Protected Health Information

The HIPAA Privacy Rule requires a covered entity with direct treatment relationships with individuals to give the NPP to every individual no later than the date of first service delivery, and to make a good faith effort to obtain the individual's written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where care is provided directly to individuals, the provider must also post

the notice in the facility in a clear and prominent location where individuals are likely to see it, as well as make the notice available to those who ask for a copy.²

We observed the current DHS NPP in a prominent location near the patient reception area, which is where visitors of the facility are most likely to see it. In addition, the NPP is available on Wilmington's website.³ Our review of the website noted that it included a link to the NPP in both English and Spanish.

Since November 1, 2014, Wilmington has maintained an electronic copy of completed NPP Acknowledgment of Receipt forms in the Online Real-time Centralized Health Information Database (ORCHID), DHS' electronic medical record system. Wilmington's Administrative Clinic Manager stated that all patients are provided with the NPP on their first service delivery date. We randomly selected and reviewed 10 patients' medical charts to determine whether Wilmington obtained patients' NPP Acknowledgments. We noted that two (20%) of the charts did not contain an NPP Acknowledgment. Upon being informed of our finding, Wilmington staff sent NPP Acknowledgment forms to the patients to be completed, returned, and scanned into ORCHID upon receipt.

DHS' NPP satisfies the HIPAA requirements, but Wilmington staff should ensure that patient acknowledgments are consistently documented and maintained.

Recommendation

- 1. Wilmington management ensure that all patients complete an Acknowledgment of Notice of Privacy Practices, maintain a copy of the Acknowledgment in each patient's electronic medical record, and periodically review a sample of records to verify compliance.**

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of PHI. A covered entity must reasonably safeguard PHI and electronic PHI (ePHI), and make reasonable efforts to prevent any intentional or unintentional use or disclosure that violates the Privacy Rule.

During our review, we observed that the computer monitors near public areas were positioned away from the public's view so that the information was not readable. Fax machines, printers, and copiers were kept in secure areas and away from visitors. It appears that the workstations are compliant with the HIPAA standards.

² Ibid., §164.520(c)

³ Ibid., §164.520(c)

Wilmington does not utilize patient sign-in sheets. Patients check-in with staff at the registration window before they are directed to the waiting area for their appointments. Patients are escorted by staff through restricted areas to examination rooms.

We observed that medical records are located in the business office, which has a security keypad and access is restricted to facility staff only. The Administrative Clinic Manager told us that medical charts are pulled daily by the medical records staff in advance of patient appointments. The Administrative Manager further told us that medical charts are returned to the medical records room before the end of the business day.

Currently, access to medical charts is manually tracked on the record folder itself, as Wilmington does not have a centralized electronic tracking system. The Coastal Health Centers' Privacy Coordinator stated that he is working with Wilmington staff to implement an electronic tracking system similar to one used by the Long Beach Comprehensive Health Center. It appears that the medical records staff are adhering to the procedures for maintaining accurate accounting of records for the facility.

The Coastal Health Centers' Privacy Coordinator stated that since November 1, 2014, Wilmington has been manually inputting hardcopy medical records into ORCHID. Hardcopy records are retrieved during a patient's first post-ORCHID-implementation visit to be input to the system, but would not be accessed again unless specifically requested by the medical provider. In November 2015, Wilmington will begin transferring hardcopy files to offsite storage.

Wilmington's Administrative Clinic Manager stated that the facility's computers are password protected and will automatically log out users after three minutes of inactivity. Passwords are changed every 90 days per DHS policy. Employees are notified and periodically reminded to not store ePHI on hard drives. Staff are granted access to ePHI by management, based on each employee's job function. ORCHID has the ability to limit access to certain fields containing ePHI based on the staff's business need and role. Thus, it appears that Wilmington is compliant with the security standards for password protections.

Wilmington has an on-site pharmacy. Per California Business and Professions Code §4116, no person other than a pharmacist, intern pharmacist, authorized officer of the law, or person authorized to prescribe shall be permitted into the area where controlled substances or dangerous drugs are stored, prepared, dispensed, etc. Wilmington's Administrative Clinic Manager stated that no one is allowed in the pharmacy unless a pharmacist is present. Thus, it appears that the pharmacy maintains physical security that is compliant with both federal and State regulations.

During our review, we noted that there is a second entrance to Wilmington designated for employees that could allow access to unsecured clinical areas that may contain

confidential information. According to Wilmington staff, the door is only open for a few hours each day to allow employees convenient access to and from the rear parking lot. However, the areas directly adjacent to the door are not actively monitored by staff, and it is possible for a patient to mistakenly enter the facility unmonitored, though we found no evidence that this has occurred.

It appears that Wilmington has generally implemented appropriate safeguards for PHI, but must secure the second entrance door.

Recommendation

- 2. Secure the second (rear) entrance door at all times, and/or implement access control measures (e.g., a keypad or proximity card, etc.) to prevent the possibility of unauthorized access/entry.**

Training

A covered entity must train all members of its workforce on policies and procedures related to PHI that are required by the HIPAA Privacy and Security Rules to the extent necessary and appropriate for the members of its workforce to carry out their functions. Members of the workforce include employees, volunteers, and trainees.⁴

During our review, we were informed that all Wilmington workforce members have received training on the HIPAA Privacy and Security Rules, HITECH Act's Breach Notification Rule, and DHS' HIPAA policies and procedures through DHS' web-based training. Initial HIPAA training is also provided by DHS' Human Resources Division during new employee orientation via a handbook format. Refresher training is provided on an as-needed basis, and during re-orientation training and employee evaluations.

We obtained a HIPAA training status report from DHS' Privacy Officer, and noted that 27 of 28 current Wilmington employees have completed DHS' HIPAA training. The remaining employee has been on long-term leave since the current HIPAA training curriculum was implemented in 2013. Therefore, it appears that Wilmington is compliant with the HIPAA training standards.

Complaint Process

A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures. A covered entity must document all complaints received, and their disposition, if any.⁵

⁴ 45 CFR § 164.530(b)

⁵ 45 CFR § 164.530(d)

According to the Coastal Health Centers' Privacy Coordinator, patients with HIPAA-related complaints are provided with a HIPAA complaint intake form. All Wilmington supervisors have access to the complaint form via Harbor-UCLA's Intranet site, and can print a copy upon request. According to DHS Policy 361.11, *Investigation of Privacy-Related Complaints Involving Alleged Violations or Breaches of Protected Health Information (PHI)*, complaints are forwarded to the Coastal Health Centers' Privacy Coordinator, who will attempt to resolve the complaints in 30 days and provide resolution to individuals in writing, if applicable. The Coastal Health Centers' Privacy Coordinator provided us with the complaint investigation process and timeline. Wilmington created a complaint log approximately three years ago, but has not received a HIPAA complaint since.

We verified through interviews and meetings that Wilmington management is aware that individuals have a right to file a complaint with DHS' Privacy Officer, the County's Chief HIPAA Privacy Officer, and/or the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR). The contact information for the above offices is provided to patients via the NPP.

It appears that Wilmington has an appropriate complaint process and policy that meet the HIPAA standards.

Refraining from Intimidating or Retaliatory Acts

Discussions with Wilmington management confirm their awareness and understanding of the requirement to adhere to DHS' Non-retaliation Policy 361.13. Further, they understand that OCR will investigate any complaint against a covered entity that asserts retaliatory actions.

Uses and Disclosures Requiring An Authorization

Guidance from OCR states that an authorization is a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual. An authorization must specify a number of elements, including a description of the PHI to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed.

Discussions with Wilmington management confirmed that workforce members have a general understanding of DHS Policy 361.3, which addresses uses and disclosures requiring an authorization from patients or their legal representatives and adhere to the policies.

Accounting for Disclosures of Protected Health Information

An individual has a right to receive an accounting of disclosures of PHI made by a covered entity. Covered entities are required to account to individuals for certain non-routine disclosures of PHI. The Privacy Rule gives individuals the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, up to six years after the disclosure. The types of disclosures that are not required to be reported are disclosures:

- to the individual
- for treatment, payment, and health care operations
- for facility directories
- pursuant to authorization
- pursuant to a limited data set agreement
- to persons involved in the individual's care
- for correctional institutions
- for certain law enforcement purposes

Wilmington management reported that all disclosures of PHI are tracked electronically via ORCHID. Wilmington management is aware that tracking for all disclosures must be maintained, with the exceptions described above, for a minimum of six years. Overall, it appears that Wilmington is complying with HIPAA requirements for accounting for disclosures of PHI.

Minimum Necessary Rule

When using, disclosing, or requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

The Privacy Rule requires covered entities to make reasonable efforts to limit the use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose of the disclosure. OCR allows covered entities flexibility to address their unique circumstances and make their own assessment of what PHI is reasonably necessary for a particular purpose.⁶

We reviewed DHS Policy 361.8, which addresses the HIPAA standards on the Minimum Necessary Rule. Discussions with Wilmington management confirm that workforce members are aware of the minimum necessary standards and adhere to them to the best of their ability.

⁶ 45 CFR § 164.502 and 514(d)

HITECH Act Breach Notification

HHS issued regulations requiring health care providers, health plans, and other entities covered by HIPAA to notify individuals when their health information is breached. These “breach notification” regulations implement provisions of the HITECH Act, passed as part of the American Recovery and Reinvestment Act of 2009. The regulations developed by OCR require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

Wilmington’s Administrative Clinic Manager stated that staff received training on breach reporting. All DHS Workforce members are required to follow DHS Policy 361.11, *Investigation of Privacy-Related Complaints Involving Alleged Violations or Breaches of Protected Health Information (PHI)*, which provides procedures for workforce members to follow when they encounter a potential privacy and/or security breach.

The Coastal Health Centers’ Privacy Coordinator told us that the Wilmington facility has not experienced a breach in at least three years. The Chief HIPAA Privacy Officer (CHPO) confirmed that the Auditor-Controller has not received a complaint or report of a breach within the past three years. However, it appears that Wilmington is aware of DHS Policy 361.11 for breach notifications.

Appropriate Access to ePHI

The Security Rule requires covered entities to have policies and procedures to ensure that workforce members have appropriate access to ePHI, and to prevent those workforce members who do not have access from obtaining access to ePHI.⁷

DHS Policy 935.15, *System Audit Controls*, addresses controls to record and examine system activity for all electronic information systems. DHS’ Privacy Officer and the Coastal Health Centers’ Privacy Coordinator stated that in order to access ORCHID, users are required to authenticate to the system, and that the system maintains session logs, rights, and other tools to ensure appropriate access to DHS’ data. The DHS Privacy Officer stated that user access is determined by the user’s role/assignment. It appears that DHS’ policy adequately addresses workforce access to ePHI.

Contingency Plan

The Security Rule includes requirements for covered entities to ensure the confidentiality, integrity, and availability of all ePHI information they create, receive,

⁷ 45 CFR § 308(a)(3)(i)

maintain, or transmit. The Security Rule further requires that covered entities protect against any reasonably anticipated threats or hazards to the security or integrity of such information. Other provisions require policies and procedures for responding to emergencies or other occurrences (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI. Contingency plans must be implemented and tested.⁸

DHS Policy 935.07, *Facility IT Contingency Plan*, details the requirements that Wilmington must follow to be compliant with HIPAA regulations. In addition, Wilmington's Administrative Clinic Manager indicated that their facility has specific workstations that will remain operational in the event of power failure or some other similar event. It appears that Wilmington is compliant with the HIPAA standards for contingency planning.

Proper Destruction of PHI

Covered entities must implement reasonable safeguards to limit incidental and prohibited uses and disclosures of PHI, including in connection with the disposal of such information. In addition, the Security Rule requires implementation of policies and procedures to address the final disposition of ePHI and/or the hardware and electronic media on which PHI is stored.

DHS Policy 935.13, *Device and Media Controls*, addresses proper disposal of ePHI. The policy states that "prior to disposal or transfer of IT resources out of DHS' inventory, all information and software containing PHI shall be rendered unreadable and unrecoverable to prevent unauthorized disclosure of DHS data."

We observed that Wilmington has locked shredding bins throughout the facility which allows for proper disposal of PHI in paper medium. Overall, it appears that Wilmington has policies and procedures in place to ensure the proper disposal of PHI.

Conclusion

We shared our findings with DHS and Wilmington management on August 18, 2015. DHS' Privacy Officer will work with Wilmington management to implement our recommendations. We will follow-up with Wilmington management in 120 days from the date of this report to ensure the deficiencies have been corrected. We thank DHS' Privacy Officer, Coastal Health Centers' Privacy Coordinator, and Wilmington's Administrative Clinic Manager and staff for their cooperation and assistance with this review.

⁸ 45 CFR § 164.308(a)

Mitchell H. Katz, M.D.
October 5, 2015
Page 10

Please call me if you have any questions, or your staff may contact Linda McBride, CHPO, at (213) 974-2166.

JN:RGC:GZ:LTM:TW

c: Chief Executive Office
County Counsel
Audit Committee
Health Deputies